

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-101984
 (43)Date of publication of application : 07.04.2000

(51)Int.Cl.

H04N 7/167
 H04H 1/02
 H04L 9/08
 H04N 7/16

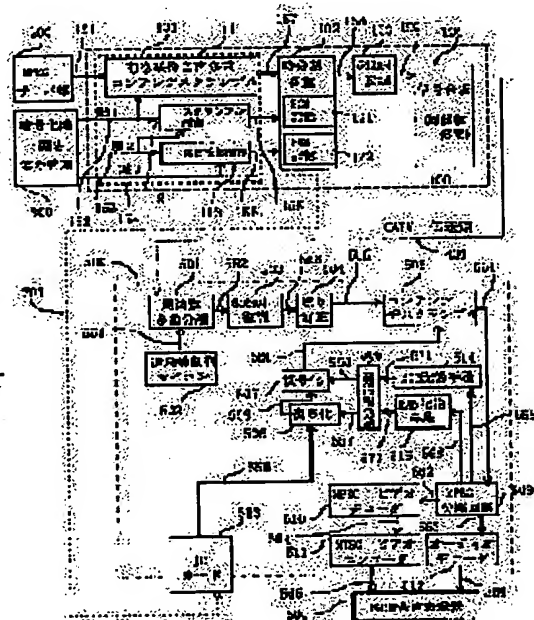
(21)Application number : 10-270113
 (22)Date of filing : 24.09.1998

(71)Applicant : HITACHI LTD
 (72)Inventor : TANAKA HIROMI
 NODA TSUTOMU
 NISHIDA MASAMI

(54) LIMITED RECEIVING SYSTEM OF CABLE TELEVISION, AND ITS TRANSMITTER AND ITS RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a transmitter-receiver whose program selection channel time is short in a limited receiving system for digital cable television.
SOLUTION: A transmitter side is provided with a multiplexer, which has digital data in a transport stream format and a function that performs time division multiplexing of ECM information and EMM information, also stores the ECM information and the EMM information and repeatedly transmits them. Receivers 500 and 600 sides are provided with an ECM storing means 514 and an EMM storing means 515 for storing the ECM information and the EMM information for every corresponding contracted channel. Scramble is released by using the information stored in these means 514 and 515, until the ECM information and the EMM information are updated.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

Best Available Copy

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-101984

(P2000-101984A)

(43) 公開日 平成12年4月7日 (2000.4.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 N 7/167		H 0 4 N 7/167	Z 5 C 0 6 4
H 0 4 H 1/02		H 0 4 H 1/02	F 5 J 1 0 4
H 0 4 L 9/08		H 0 4 N 7/16	C
H 0 4 N 7/16		H 0 4 L 9/00	6 0 1 A
			6 0 1 B

審査請求 未請求 請求項の数24 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平10-270113

(22) 出願日 平成10年9月24日 (1998.9.24)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 田中 大幹

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所AV事業部内

(72) 発明者 野田 勉

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所マルチメディアシステム開発本部内

(74) 代理人 100061893

弁理士 高橋 明夫 (外1名)

最終頁に続く

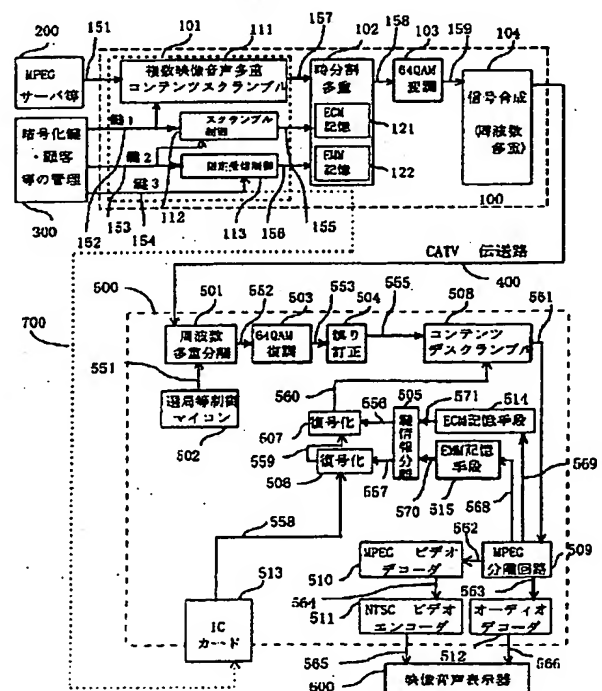
(54) 【発明の名称】 ケーブルテレビの限定受信システム並びその送信装置及びその受信装置

(57) 【要約】

【課題】 デジタルケーブルテレビの限定受信システムにおいて、番組選局時間の短い送受信装置を提供することにある。

【解決手段】 送信装置側ではトランスポートストリーム形式のデジタルデータとECM情報やEMM情報を時分割多重すると共にECM情報およびEMM情報を記憶して繰り返し送出する機能を有する多重化装置を備え、受信装置側では対応する契約チャンネル毎にECM情報及びEMM情報をを記憶するECM記憶手段とEMM記憶手段とを備え、ECM情報およびEMM情報が更新されるまではこのECM記憶手段及びEMM記憶手段に記憶された情報を用いてスクランブルを解除する。

図 1



Best Available Copy

【特許請求の範囲】

【請求項 1】第 1 の鍵データを第 2 の鍵データによって暗号化する手段、第 2 の鍵データを第 3 の鍵データによって暗号化する手段、前記暗号化された第 1 の鍵データによって送信するコンテンツデータをスクランブルする手段、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第 1 の鍵データを含む E C M 情報及び暗号化された前記第 2 の鍵データを含む E M M 情報を時分割多重する手段、前記時分割多重手段に設けられた前記 E C M 情報を繰り返し出力するための E C M 記憶手段、前記時分割多重手段の出力を変調する手段を備えた送信装置と、

前記デジタル変調されたコンテンツデータ、前記 E C M 情報、前記 E M M 情報を復調する手段、第 3 の鍵データの出力手段、前記 E C M 情報及び復号された前記第 1 の鍵データのいずれか一方を記憶する第 1 の記憶手段、前記 E M M 情報及び復号された前記第 2 の鍵データのいずれか一方を記憶する第 2 の記憶手段、暗号化された前記第 2 の鍵データを前記第 3 の鍵データを用いて復号する第 2 の鍵データ復号手段、暗号化された前記第 1 の鍵データを前記復号された第 2 の鍵データを用いて復号する第 1 の鍵データ復号手段、復号された前記第 1 の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第 1、前記第 2 の記憶手段の出力を用いてスクランブルを解除する受信装置と、から構成されることを特徴とするケーブルテレビの限定受信システム。

【請求項 2】請求項 1 記載のケーブルテレビの限定受信システムにおいて、前記送信装置の前記時分割多重手段に E M M 情報を繰り返し出力するための E M M 記憶手段を設けることを特徴とするケーブルテレビの限定受信システム。

【請求項 3】請求項 1 記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第 1 の記憶手段は E C M 情報を記憶し、前記第 2 の記憶手段は E M M 情報を記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項 4】請求項 1 記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第 1 の記憶手段は復号された第 1 の鍵データを記憶し、前記第 2 の記憶手段は復号された第 2 の鍵データを記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項 5】請求項 1 記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第 1 の記憶手段には E C M 情報を記憶し、前記第 2 の記憶手段には復号された第 2 の鍵データを記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項 6】第 1 の鍵データを第 2 の鍵データによって暗号化する手段と、第 2 の鍵データを第 3 の鍵データに

よって暗号化する手段と、暗号化された前記第 1 の鍵データによって送信するコンテンツデータをスクランブルする手段と、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第 1 の鍵データを含む E C M 情報及び暗号化された前記第 2 の鍵データを含む E M M 情報を時分割多重する手段と、前記時分割多重手段に設けられ、前記 E C M 情報を繰り返し出力するための E C M 記憶手段と、前記時分割多重手段の出力を変調して送信する手段とを備えることを特徴とするケーブルテレビの送信装置。

【請求項 7】請求項 6 記載の送信装置において、前記送信装置の前記時分割多重手段に前記 E M M 情報を繰り返し出力するための E M M 記憶手段を設けることを特徴とするケーブルテレビの送信装置。

【請求項 8】送信装置から送付されたスクランブルされたコンテンツデータ、E C M 情報、E M M 情報からコンテンツデータのスクランブルを解除するために、第 3 の鍵データの出力手段と、前記 E C M 情報及び復号された前記第 1 の鍵データのいずれか一方を記憶する第 1 の記憶手段と、前記 E M M 情報及び復号された前記第 2 の鍵データのいずれか一方を記憶する第 2 の記憶手段と、暗号化された前記第 2 の鍵データを前記第 3 の鍵データを用いて復号する第 2 の鍵データ復号手段と、暗号化された前記第 1 の鍵データを前記復号された第 2 の鍵データを用いて復号する第 1 の鍵データ復号手段と、復号された前記第 1 の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第 1、前記第 2 の記憶手段の出力を用いてスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項 9】請求項 8 記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第 1 の記憶手段は前記 E C M 情報を記憶し、前記第 2 の記憶手段は前記 E M M 情報を記憶することを特徴とするケーブルテレビの受信装置。

【請求項 10】請求項 8 記載のケーブルテレビの受信装置において、前記受信装置の前記第 1 の記憶手段は復号された第 1 の鍵データを記憶し、前記第 2 の記憶手段は復号された第 2 の鍵データを記憶することを特徴とするケーブルテレビの受信装置。

【請求項 11】請求項 8 記載のケーブルテレビの受信装置において、前記受信装置の前記第 1 の記憶手段は E C M 情報を記憶し、前記第 2 の記憶手段は復号された第 2 の鍵データを記憶することを特徴とするケーブルテレビの受信装置。

【請求項 12】請求項 8 記載のケーブルテレビの受信装置において、前記第 1 の記憶手段の出力を用いて前記スクランブル解除手段でコンテンツデータのスクランブルが解除されない場合には、送信されてきた E C M 情報を用いて前記第 1 の記憶手段を更新し、前記第 1 の記憶手

段の出力を用いてコンテンツデータのスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項13】請求項8記載のケーブルテレビの受信装置において、前記第2の記憶手段の出力を用いて前記第1の鍵データの復号ができない場合には、送信されてきたECM情報で前記第2の記憶手段を更新し、前記更新された第2の記憶手段の出力を用いて前記第1の鍵データを復号することを特徴とするケーブルテレビの受信装置。

【請求項14】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第1の鍵データの暗号化されたデータを含むECM情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第1の鍵データの暗号化を解除する場合に必要な第2の鍵データを含むECM情報を生成する限定受信制御装置、

第2の鍵データの暗号化を解除するために必要となる第3の鍵データ及び前記第1、前記第2の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記ECM情報や前記ECM情報を時分割多重すると共に前記ECM情報及び前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、

を備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ECM情報より前記第1の鍵データを復号する第1の鍵データ復号手段、

前記復調手段で得られた前記ECM情報より前記第2の鍵データを復号する第2の鍵データ復号手段、

前記ECM情報を対応する契約チャンネル毎に記憶するECM記憶手段、

前記ECM情報を対応する契約チャンネル毎に記憶するECM記憶手段、

前記復調手段で得られたコンテンツスクランブルのかかった前記データから前記第1の鍵データ復号手段で得られた第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、

を備えた受信装置と、

から構成され、ECM情報に変更があるまでは契約チャンネルを選局する毎に前記ECM記憶手段に記憶したE

CM情報を利用して、このデータを一旦前記第1の鍵データ復号手段において復号することにより前記第1の鍵データを抽出し、この抽出した前記第1の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかった前記データより前記デスクランブル手段によって前記トランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項15】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第1の鍵データの暗号化されたデータを含むECM情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第1の鍵データの暗号化を解除する場合に必要な第2の鍵データを含むECM情報を生成し多重化装置へ出力する限定受信制御装置、

前記第2の鍵データの暗号化を解除するために必要となる第3の鍵データ、前記第1、前記第2の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記ECM情報や前記ECM情報を時分割多重すると共に前記ECM情報及び前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた前記ECM情報より前記第1の鍵データを復号する第1の鍵データ復号手段、

前記復調手段で得られた前記ECM情報より前記第2の鍵データを復号する第2の鍵データ復号手段、

前記第1の鍵データ復号手段によって復号された前記第1の鍵データ自体を対応する契約チャンネル毎に記憶する第1の鍵データ記憶手段、

前記第2の鍵データ復号手段によって復号された前記第2の鍵データ自体を対応する契約チャンネル毎に記憶する第2の鍵データ記憶手段、

前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ECM復号手段から得られた復号化された前記第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、

とを備えた受信装置と、

から構成され、前記ECM情報または前記ECM情報に

変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用して前記デスクランブル手段によって前記復調手段で得られたコンテンツスクランブルのかかったデータからトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項 16】暗号化されたトランスポートストリーム形式のデジタルデータを送信するために、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段と、受信側でコンテンツのスクランブルを解除するために必要となる第 1 の鍵データの暗号化されたデータを含む ECM 情報を生成しスクランブル装置を制御するスクランブル制御装置と、前記第 1 の鍵データの暗号化を解除する場合に必要な第 2 の鍵データを含む EMM 情報を生成し多重化装置へ出力する限定受信制御装置と、前記第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ、前記第 1、前記第 2 の鍵データ及び顧客情報を管理する鍵情報管理装置と、トランスポートストリーム形式のデジタルデータと前記 ECM 情報や前記 EMM 情報を時分割多重すると共に前記 ECM 情報及び前記 EMM 情報を記憶して繰り返し送出する機能を有する多重化装置と、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段と、複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備えることを特徴とするケーブルテレビの送信装置。

【請求項 17】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた ECM 情報より第 1 の鍵データを復号する第 1 の鍵データ復号手段と、前記復調手段で得られた EMM 情報より第 2 の鍵データを復号する第 2 の鍵データ復号手段と、前記 ECM 情報を対応する契約チャンネル毎に記憶する ECM 記憶手段と、前記 EMM 情報を記憶する EMM 記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第 1 の鍵データ復号手段で得られた第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えることを特徴とするケーブルテレビの受信装置。

【請求項 18】請求項 17 記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記 ECM 記憶手段に記憶された ECM 情報を用いて前記第 1 の鍵データを復号して前記デスクランブル手段に供給し、前記第 1 の鍵データでデスクランブル処理がされない場合には前記復調手段から新しく ECM 情報を抽出して前記 ECM 記憶手段に記憶された ECM 情報を更新し、更新された ECM 情報によって第 1 の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除することを特徴とするケーブルテレビの受信装置。

【請求項 19】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた ECM 情報より第 1 の鍵データを復号する第 1 の鍵データ復号手段と、前記復調手段で得られた EMM 情報より第 2 の鍵データを復号する第 2 の鍵データ復号手段と、前記第 1 の鍵データ復号手段によって復号された前記第 1 の鍵データ自体を対応する契約チャンネル毎に記憶する第 1 の鍵データ記憶手段と、前記第 2 の鍵データ復号手段によって復号された前記第 2 の鍵データ自体を対応する契約チャンネル毎に記憶する第 2 の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記 ECM 復号手段で得られた鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えたことを特徴とするケーブルテレビの受信装置。

【請求項 20】請求項 19 記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記第 1 の鍵データ記憶手段に記憶された前記第 1 の鍵データを前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しく ECM 情報を抽出して前記第 1 の鍵データ復号手段によって第 1 の鍵データを復号して前記第 1 の鍵データ記憶手段に記憶された第 1 の鍵データを更新し、前記更新された第 1 の鍵データを前記デスクランブル手段に供給してスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項 21】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第 1 の鍵データの暗号化されたデータを含む ECM 情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第 1 の鍵データの暗号化を解除する場合に必要な第 2 の鍵データを含む EMM 情報を生成し多重化装置へ出力する限定受信制御装置、

前記第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ、前記第 1、前記第 2 の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記 ECM 情報や前記 EMM 情報を時分割多重すると共に前記 ECM 情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、

とを備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記 E C M 情報より前記第 1 の鍵データを復号する第 1 の鍵データ復号手段、

前記復調手段で得られた前記 E M M 情報より前記第 2 の鍵データを復号する第 2 の鍵データ復号手段、

前記 E C M 情報を対応する契約チャンネル毎に記憶する E C M 記憶手段、

前記 E M M 情報を対応する契約チャンネル毎に記憶する E M M 記憶手段、

前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第 1 の鍵データ復号手段で得られた前記第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、

とを備えた受信装置と、

から構成され、前記 E C M 情報に変更があるまでは契約チャンネルを選局する毎に前記 E C M 記憶手段に記憶した前記 E C M 情報を利用するために、このデータを一旦前記第 1 の鍵データ復号手段で復号して前記第 1 の鍵データを抽出し、この抽出された前記第 1 の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項 2 2】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、

受信側でコンテンツのスクランブルを解除するために必要となる第 1 の鍵データの暗号化されたデータを含む E C M 情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第 1 の鍵データの暗号化を解除する場合に必要な第 2 の鍵データを含む E M M 情報を生成し多重化装置へ出力する限定受信制御装置、

前記第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ、前記第 1、前記第 2 の鍵データ及び

顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記 E C M 情報や前記 E M

M 情報を時分割多重すると共に前記 E C M 情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、

とを備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段、

前記復調手段で得られた前記 E C M 情報より前記第 1 の鍵データを復号する第 1 の鍵データ復号手段、

前記復調手段で得られた前記 E M M 情報より前記第 2 の鍵データを復号する第 2 の鍵データ復号手段、

前記 E C M 情報を対応する契約チャンネル毎に記憶する E C M 記憶手段、

前記第 2 の鍵データ復号手段によって復号された前記第 2 の鍵データ自体を対応する契約チャンネル毎に記憶する第 2 の鍵データ記憶手段、

10 前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第 1 の鍵データ復号手段で得られた前記第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、とを備えた受信装置と、

から構成され、前記 E C M 情報に変更があるまでは契約チャンネルを選局する毎に前記 E C M 記憶手段に記憶した前記 E C M 情報を利用すると共に、前記 E M M 情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用するために、このデータを一旦前記第 1 の鍵データ復号手段で復号して前記第 1 の鍵データを抽出し、この抽出された前記第 1 の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項 2 3】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた E C M 情報より第 1 の鍵データを復号する第 1 の鍵データ復号手段と、前記復調手段で得られた E M M 情報より第 2 の鍵データを復号する第 2 の鍵データ復号手段と、前記 E C M 情報を対応する契約チャンネル毎に記憶する E C M 記憶手段と、前記第 2 の鍵データ復号手段によって復号された前記第 2 の鍵データ自体を対応する契約チャンネル毎に記憶する第 2 の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第 1 の鍵データ復号手段で得られた第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えることを特徴とするケーブルテレビの受信装置。

【請求項 2 4】請求項 2 3 記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記 E C M 記憶手段に記憶された E C M 情報を用いて前記第 1 の鍵データを復号して前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しく E C M 情報を抽出して前記 E C M 記憶手段に記憶された前記 E C M 情報を更新し、その更新された E C M 情報によって第 1 の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除をすることを特徴とするケーブルテレビの受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、テレビジョン放送の受信者を特定して受信を許可する限定受信方式に関わり、特にCATV (Cable Television) 伝送路などを使用したデジタル有線テレビジョン放送の限定受信システム並びにその送信装置及びその受信装置に関するものである。

【0002】

【従来の技術】従来、ケーブルテレビと呼ばれるCATV伝送路を使用したテレビジョン放送における限定受信方式については、コロナ社発行、(社)電子機械工業会ケーブルテレビ技術委員会編「ケーブルテレビ技術入門」に記述されている。その記述によれば、1WAYアドレサブルシステムと呼ばれる方式が記述されている。この方式は、受信側ホームターミナル内のデスクランブル機能を送信側からのFSK (Frequency Shift Keying) 変調の下り回線で制御している。そのスクランブルシステムの詳細な記述はないが、以下の経緯で限定受信方式が進歩しながら変わってきている。まず、簡単な限定受信方式として、映像信号を伝送しているチャンネル以外の帯域でFSK変調などで伝送される下り回線の制御情報によってCATV受信機の選局を制限する俗称チャンネルスキップ方式があった。そのチャンネルスキップ方式は、受信者が契約していないチャンネルを受信できないように、CATV受信機が下り回線の制御情報に応じて受信可能だが、契約していないチャンネルを飛ばすものである。ところが、CATVチャンネル対応テレビ受像機が一般ユーザーへ販売されるようになって、チャンネルを飛ばすことができなくなり、限定受信の機能がなくなった。

【0003】他の限定受信方式として、同期圧縮のスクランブル方式がある。この方式では、NTSC (National Television Committee) 映像信号の水平同期信号の期間をレベルを少なくして送信することで、CATVチャンネル対応テレビ受像機でも再生できなくなった。CATV受信機では、受信者が契約しているチャンネルを受信する場合には、レベルが圧縮されて小さくされた水平同期信号の振幅を下り回線の制御情報、すなわちキー情報に応じてこの水平同期信号を伸長して正規のレベルまで戻すことによって、契約チャンネルを再生できる。この同期圧縮のスクランブル方式がNTSC映像を伝送するアナログテレビジョン放送の限定受信方式として一般的であるが、デジタル有線テレビジョン放送の限定受信方式については記述されていない。

【0004】また、最近のデジタル伝送技術などの発展に伴い、アナログ信号であるNTSC映像の伝送チャンネル1チャンネルで複数のデジタル化された映像を伝送することが計画されている。このケーブルテレビのデジ

タル伝送については、1995年9月21日に発表されたテレビジョン学会技術報告 (vol. 19, No. 42) 19頁から24頁の「電気通信技術審議会暫定方式デジタル有線テレビジョン放送伝送実験」に記載されている。この報告によれば、エムペグ2 (MPEG2: Moving Picture Expert Group phase 2) と呼ばれるデジタル画像圧縮技術によって圧縮された画像などのデジタルデータが多重されたトランスポートストリームと呼ばれる形式のデータ列にされ、リードソロモン誤り訂正などの信号処理をされた後、64QAM (Quadrature Amplitude Modulation: 64値直交振幅変調) と呼ばれるデジタル変調技術によって変調されてCATV伝送路で伝送される。この報告でも、デジタルCATVの限定受信方式については記述されていない。

【0005】一方、多チャンネルのデジタル化された映像を配信する方式としてデジタル衛星テレビジョン放送があり、その放送については、日経エレクトロニクス1996年9月2日号149頁の論文「70近くの多チャンネルを実現する日本初のデジタル衛星放送」に記載されているように、デジタル画像圧縮技術とデジタル伝送技術の組み合わせによって実現している。この論文によれば、日本独自のスクランブルシステムとICカード (半導体メモリ内蔵カード) によるスクランブル解除によって、受信者を特定して受信許可する限定受信方式を実現している。このように、衛星テレビジョン放送は、衛星を介した放送のため各家庭から送信側に情報を送る上り回線は、ICカードや電話回線を用いたシステムとなっている。この論文では、スクランブルシステムとICカードによるスクランブル解除の限定受信方式をデジタル有線テレビジョン放送など他の伝送方式に適應するための記述が無い。

【0006】また、ケーブルテレビのデジタルテレビジョン放送における限定受信方式については、(社)日本CATV技術協会 規格・標準化委員会において標準化方式が検討され、1997年4月に規格書JCTEA STD001-1.0が発行された。それによると、この衛星テレビジョン放送に類似の方式で、送信側では映像や音声などのトランスポートストリームデータを第1の鍵データによりスクランブルし、その後第2の鍵データにより暗号化した第1の鍵データをECM (Entitlement Control Message) 情報に入れてこれを多重器によってこの第1の鍵データによってスクランブルされた映像や音声などのトランスポートストリームデータと時分割多重する。また、第2の鍵データは第3の鍵データにより暗号化され、その後ECM (Entitlement Management Message) 情報に入れてこれを多重器によってこの第1の鍵データによってスクランブルされた映像や音声およびこのECM情報 (以下単にECMと云う) など

のトランスポートストリームデータと時分割多重して送出する。この出力データストリームを64QAMなどのデジタル変調する変調手段により変調し、信号合成手段により複数の被変調波を周波数多重して伝送路に送出する。ここで第3の鍵データはICカードなどに記憶させておく方法などが考えられている。一方受信側では周波数多重されて伝送された64値などの多値QAMなどのデジタル被変調波を復調手段により復調し、誤り訂正を施した後、MPEG分離回路で多重されているトランスポートストリームを分離する。この時ECM情報およびEMM情報を検出し、予め与えられた第3の鍵データを用いてEMM情報（以下単にEMMと云う）に含まれている第2の鍵データを復号し、復号した第2の鍵データを用いてECM情報に含まれている第1の鍵データを復号する。この第1の鍵データを用いることでスクランブルされた映像や音声の復号することが可能となる。復号された映像や音声のトランスポートストリームはMPEG分離回路で分離されそれぞれデコードICを通して再生される。但し、この時のECM情報およびEMM情報のビット単位の構成に関してはなんら規定はされていない。また、送信側におけるECM情報およびEMM情報の送出頻度も任意とされている。

【0007】

【発明が解決しようとする課題】従来の技術では、CATV伝送路を使用したデジタル有線テレビジョン放送に関する限定受信方式の詳細な技術は公開されていない。しかしながら現在までに規格化されている事項から考えると、CATVの送信側におけるECM情報およびEMM情報の送出頻度も任意とされている。その方式によれば、受信機側に於いてスクランブルの施されたチャンネルを選ぶいわゆる選局動作をする場合には、受信機がECM情報を受け取った時点で初めてスクランブルを解くことができるため、受信機の選局から映像や音声のスクランブルを解かれて出力するまでのいわゆる選局動作とECM情報の送出頻度が密接に関係していた。そのため、受信機の選局動作を早くするためにはECM情報の送出頻度を上げる必要があった。しかし、送出頻度を上げるとECM情報の伝送容量が増えるので、同時に多重される映像や音声などのトランスポートストリームの伝送容量を圧迫してしまうといった問題が考えられる。

【0008】本発明の目的は上記の欠点を解決したケーブルテレビの限定受信システム並びにその送信装置及びその受信装置を提供することにある。本発明の他の目的は受信装置での選局に要する時間を短縮することができるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置を提供することにある。

【0009】

【課題を解決するための手段】本発明の目的を達成するために、本発明によるケーブルテレビの限定受信システムは、第1の鍵データを第2の鍵データによって暗号化

する手段、第2の鍵データを第3の鍵データによって暗号化する手段、前記暗号化された第1の鍵データによって送信するコンテンツデータをスクランブルする手段、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第1の鍵データを含むECM情報及び暗号化された前記第2の鍵データを含むEMM情報を時分割多重する手段、前記時分割多重手段に設けられた前記ECM情報を繰り返し出力するためのECM記憶手段、前記時分割多重手段の出力を変調する手段を備えた送信装置と、前記デジタル変調されたコンテンツデータ、前記ECM情報、前記EMM情報を復調する手段、第3の鍵データの出力手段、前記ECM情報及び復号された前記第1の鍵データのいずれか一方を記憶する第1の記憶手段、前記EMM情報及び復号された前記第2の鍵データのいずれか一方を記憶する第2の記憶手段、暗号化された前記第2の鍵データを前記第3の鍵データを用いて復号する第2の鍵データ復号手段、暗号化された前記第1の鍵データを前記復号された第2の鍵データを用いて復号する第1の鍵データ復号手段、復号された前記第1の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第1、前記第2の記憶手段の出力を用いてスクランブルを解除する受信装置と、から構成される。

【0010】このケーブルテレビの限定受信システムにおいて、前記送信装置の前記時分割多重手段にEMM情報を繰り返し出力するためのEMM記憶手段を設ける。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第1の記憶手段はECM情報を記憶し、前記第2の記憶手段はEMM情報を記憶する。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第1の記憶手段は復号された第1の鍵データを記憶し、前記第2の記憶手段は復号された第2の鍵データを記憶する。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第1の記憶手段にはECM情報を記憶し、前記第2の記憶手段には復号された第2の鍵データを記憶する。

【0011】本発明の目的を達成するために、本発明のケーブルテレビの送信装置は、第1の鍵データを第2の鍵データによって暗号化する手段と、第2の鍵データを第3の鍵データによって暗号化する手段と、暗号化された前記第1の鍵データによって送信するコンテンツデータをスクランブルする手段と、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第1の鍵データを含むECM情報及び暗号化された前記第2の鍵データを含むEMM情報を時分割多重手段と、前記時分割多重手段に設けられ、前記ECM情報を繰り返し出力するためのECM記憶手段と、前記時分割多重手段の出力を変調して送信する手段とを備えている。また、この送信装置に

において、前記送信装置の前記時分割多重手段に前記 EMM 情報を繰り返し出力するための EMM 記憶手段を設ける。

【0012】本発明の目的を達成するために、本発明のケーブルテレビ受信装置は、送信装置から送付されたスクランブルされたコンテンツデータ、ECM 情報、EMM 情報からコンテンツデータのスクランブルを解除するために、第 3 の鍵データの出力手段と、前記 ECM 情報及び復号された前記第 1 の鍵データのいずれか一方を記憶する第 1 の記憶手段と、前記 EMM 情報及び復号された前記第 2 の鍵データのいずれか一方を記憶する第 2 の記憶手段と、暗号化された前記第 2 の鍵データを前記第 3 の鍵データを用いて復号する第 2 の鍵データ復号手段と、暗号化された前記第 1 の鍵データを前記復号された第 2 の鍵データを用いて復号する第 1 の鍵データ復号手段と、復号された前記第 1 の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第 1、前記第 2 の記憶手段の出力を用いてスクランブルを解除する。

【0013】このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第 1 の記憶手段は前記 ECM 情報を記憶し、前記第 2 の記憶手段は前記 EMM 情報を記憶する。また、このケーブルテレビの受信装置において、前記受信装置の前記第 1 の記憶手段は復号された第 1 の鍵データを記憶し、前記第 2 の記憶手段は復号された第 2 の鍵データを記憶する。また、このケーブルテレビの受信装置において、前記受信装置の前記第 1 の記憶手段は ECM 情報を記憶し、前記第 2 の記憶手段は復号された第 2 の鍵データを記憶する。また、このケーブルテレビの受信装置において、前記第 1 の記憶手段の出力を用いて前記スクランブル解除手段でコンテンツデータのスクランブルが解除されない場合には、送信されてきた ECM 情報を用いて前記第 1 の記憶手段を更新し、前記第 1 の記憶手段の出力を用いてコンテンツデータのスクランブルを解除する。また、このケーブルテレビの受信装置において、前記第 2 の記憶手段の出力を用いて前記第 1 の鍵データの復号ができない場合には、送信されてきた EMM 情報で前記第 2 の記憶手段を更新し、前記更新された第 2 の記憶手段の出力を用いて前記第 1 の鍵データを復号する。

【0014】本発明の目的を達成するために、本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第 1 の鍵データの暗号化されたデータを含む ECM 情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第 1 の鍵データの暗号化を解除する場合に必要となる第 2 の鍵データを含む EMM 情報を生成し多重化装置へ出力する限定受信制御装置、前記第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ、前記第 1、前記第 2 の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記 ECM 情報や前記 EMM 情報を時分割多重すると共に前記 ECM 情報及び前記 EMM 情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段を備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記 ECM 情報より前記第 1 の鍵データを復号する第 1 の鍵データ復号手段、前記復調手段で得られた前記 EMM 情報より前記第 2 の鍵データを復号する第 2 の鍵データ復号手段、前記 ECM 情報を対応する契約チャンネル毎に記憶する ECM 記憶手段、前記 EMM 情報を対応する契約チャンネル毎に記憶する EMM 記憶手段、前記復調手段で得られたコンテンツスクランブルのかかった前記データから前記第 1 の鍵データ復号手段で得られた第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、を備えた受信装置と、から構成され、ECM 情報に変更があるまでは契約チャンネルを選局する毎に前記 ECM 記憶手段に記憶した ECM 情報を利用して、このデータを一旦前記第 1 の鍵データ復号手段において復号することにより前記第 1 の鍵データを抽出し、この抽出した前記第 1 の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかった前記データより前記デスクランブル手段によって前記トランスポートストリーム形式のデジタルデータを得る。

第 2 の鍵データを含む EMM 情報を生成する限定受信制御装置、第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ及び前記第 1、前記第 2 の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記 ECM 情報や前記 EMM 情報を時分割多重すると共に前記 ECM 情報及び前記 EMM 情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段を備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記 ECM 情報より前記第 1 の鍵データを復号する第 1 の鍵データ復号手段、前記復調手段で得られた前記 EMM 情報より前記第 2 の鍵データを復号する第 2 の鍵データ復号手段、前記 ECM 情報を対応する契約チャンネル毎に記憶する ECM 記憶手段、前記 EMM 情報を対応する契約チャンネル毎に記憶する EMM 記憶手段、前記復調手段で得られたコンテンツスクランブルのかかった前記データから前記第 1 の鍵データ復号手段で得られた第 1 の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、を備えた受信装置と、から構成され、ECM 情報に変更があるまでは契約チャンネルを選局する毎に前記 ECM 記憶手段に記憶した ECM 情報を利用して、このデータを一旦前記第 1 の鍵データ復号手段において復号することにより前記第 1 の鍵データを抽出し、この抽出した前記第 1 の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかった前記データより前記デスクランブル手段によって前記トランスポートストリーム形式のデジタルデータを得る。

【0015】また、本発明による限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第 1 の鍵データの暗号化されたデータを含む ECM 情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第 1 の鍵データの暗号化を解除する場合に必要となる第 2 の鍵データを含む EMM 情報を生成し多重化装置へ出力する限定受信制御装置、前記第 2 の鍵データの暗号化を解除するために必要となる第 3 の鍵データ、前記第 1、前記第 2 の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記 ECM 情報や前記 EMM 情報を時分割多重すると共に前記 ECM 情報及び前記 EMM 情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重

して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた前記ECM情報より前記第1の鍵データを復号する第1の鍵データ復号手段、前記復調手段で得られた前記ECM情報より前記第2の鍵データを復号する第2の鍵データ復号手段、前記第1の鍵データ復号手段によって復号された前記第1の鍵データ自体を対応する契約チャンネル毎に記憶する第1の鍵データ記憶手段、前記第2の鍵データ復号手段によって復号された前記第2の鍵データ自体を対応する契約チャンネル毎に記憶する第2の鍵データ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ECM復号手段から得られた復号化された前記第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、とを備えた受信装置と、から構成され、前記ECM情報または前記ECM情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用して前記デスクランブル手段によって前記復調手段で得られたコンテンツスクランブルのかかったデータからトランスポートストリーム形式のデジタルデータを得る。

【0016】本発明によるケーブルテレビの送信装置は、暗号化されたトランスポートストリーム形式のデジタルデータを送信するために、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段と、受信側でコンテンツのスクランブルを解除するために必要となる第1の鍵データの暗号化されたデータを含むECM情報を生成しスクランブル装置を制御するスクランブル制御装置と、前記第1の鍵データの暗号化を解除する場合に必要な第2の鍵データを含むECM情報を生成し多重化装置へ出力する限定受信制御装置と、前記第2の鍵データの暗号化を解除するために必要となる第3の鍵データ、前記第1、前記第2の鍵データ及び顧客情報を管理する鍵情報管理装置と、トランスポートストリーム形式のデジタルデータと前記ECM情報や前記ECM情報を時分割多重すると共に前記ECM情報及び前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置と、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段と、複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備えている。

【0017】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたECM情報より第1の鍵データを復号する第1の鍵データ復号手段と、前記復調手段で得られたECM情報より第2の鍵データを復号する第2の鍵データ復号手段と、前記ECM情報に対応する契約チャンネル毎に記憶するECM記憶手段と、前記ECM情報を記憶するECM記憶手段と、前記復調手段で得られたコンテンツスクランブルのか

ったデータから前記第1の鍵データ復号手段で得られた第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えている。

【0018】このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ECM記憶手段に記憶されたECM情報を用いて前記第1の鍵データを復号して前記デスクランブル手段に供給し、前記第1の鍵データでデスクランブル処理がされない場合には前記復調手段から新しくECM情報を抽出して前記ECM記憶手段に記憶されたECM情報を更新し、更新されたECM情報によって第1の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除する。

【0019】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたECM情報より第1の鍵データを復号する第1の鍵データ復号手段と、前記復調手段で得られたECM情報より第2の鍵データを復号する第2の鍵データ復号手段と、前記第1の鍵データ復号手段によって復号された前記第1の鍵データ自体を対応する契約チャンネル毎に記憶する第1の鍵データ記憶手段と、前記第2の鍵データ復号手段によって復号された前記第2の鍵データ自体を対応する契約チャンネル毎に記憶する第2の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ECM復号手段で得られた鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えている。

【0020】このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記第1の鍵データ記憶手段に記憶された前記第1の鍵データを前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくECM情報を抽出して前記第1の鍵データ復号手段によって第1の鍵データを復号して前記第1の鍵データ記憶手段に記憶された第1の鍵データを更新し、前記更新された第1の鍵データを前記デスクランブル手段に供給してスクランブルを解除する。

【0021】本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第1の鍵データの暗号化されたデータを含むECM情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第1の鍵データの暗号化を解除する場合に必要な第2の鍵データを含むECM情報を生成し多重化装置へ出力する限定受信制御装置、前記

第2の鍵データの暗号化を解除するために必要となる第3の鍵データ、前記第1、前記第2の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ECM情報や前記EMM情報を時分割多重すると共に前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ECM情報より前記第1の鍵データを復号する第1の鍵データ復号手段、前記復調手段で得られた前記EMM情報より前記第2の鍵データを復号する第2の鍵データ復号手段、前記ECM情報を対応する契約チャンネル毎に記憶するECM記憶手段、前記EMM情報を対応する契約チャンネル毎に記憶するEMM記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第1の鍵データ復号手段で得られた前記第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、とを備えた受信装置と、から構成され、前記ECM情報に変更があるまでは契約チャンネルを選局する毎に前記ECM記憶手段に記憶した前記ECM情報を利用するために、このデータを一旦前記第1の鍵データ復号手段で復号して前記第1の鍵データを抽出し、この抽出された前記第1の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得る。

【0022】本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第1の鍵データの暗号化されたデータを含むECM情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第1の鍵データの暗号化を解除する場合に必要となる第2の鍵データを含むEMM情報を生成し多重化装置へ出力する限定受信制御装置、前記第2の鍵データの暗号化を解除するために必要となる第3の鍵データ、前記第1、前記第2の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ECM情報や前記EMM情報を時分割多重すると共に前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する

復調手段、前記復調手段で得られた前記ECM情報より前記第1の鍵データを復号する第1の鍵データ復号手段、前記復調手段で得られた前記EMM情報より前記第2の鍵データを復号する第2の鍵データ復号手段、前記ECM情報を対応する契約チャンネル毎に記憶するECM記憶手段、前記第2の鍵データ復号手段によって復号された前記第2の鍵データ自体を対応する契約チャンネル毎に記憶する第2の鍵データ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第1の鍵データ復号手段で得られた前記第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、を備えた受信装置と、から構成され、前記ECM情報に変更があるまでは契約チャンネルを選局する毎に前記ECM記憶手段に記憶した前記ECM情報を利用すると共に、前記EMM情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用するために、このデータを一旦前記第1の鍵データ復号手段で復号して前記第1の鍵データを抽出し、この抽出された前記第1の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得る。

【0023】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたECM情報より第1の鍵データを復号する第1の鍵データ復号手段と、前記復調手段で得られたEMM情報より第2の鍵データを復号する第2の鍵データ復号手段と、前記ECM情報を対応する契約チャンネル毎に記憶するECM記憶手段と、前記第2の鍵データ復号手段によって復号された前記第2の鍵データ自体を対応する契約チャンネル毎に記憶する第2の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第1の鍵データ復号手段で得られた第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備える。このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ECM記憶手段に記憶されたECM情報を用いて前記第1の鍵データを復号して前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくECM情報を抽出して前記ECM記憶手段に記憶された前記ECM情報を更新し、その更新されたECM情報によって第1の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除をする。

【0024】また、上記目的を達成するために、本発明においては、送信側では映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段とコンテンツのスクランブルを解除するために必要となる第1の鍵データを含むECM情報

を生成しスクランブル装置を制御するスクランブル制御装置と同じくコンテンツのスクランブルを解除するために必要となる第2の鍵データを含むECM情報を生成し多重化装置へ出力する限定受信制御装置とトランスポートストリーム形式のデジタルデータとECM情報やECM情報を時分割多重すると共に前記ECM情報を記憶して繰り返し送出する機能を有する多重化装置と前記スクランブル制御装置の出力データストリームを64値などの多値QAMなどのデジタル変調する変調手段と複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備え、受信側では周波数多重されて伝送された64値などの多値QAMなどのデジタル被変調波を復調する復調手段と、前記復調手段で得られたECM情報に対応する契約チャンネル毎に記憶するECM記憶手段と前記ECM情報の中から第1の鍵データを復号する第1の鍵データ復号手段と前記復調手段で得られたECM情報を対応する契約チャンネル毎に記憶するECM記憶手段と前記ECM情報の中から第2の鍵データを復号する第2の鍵データ復号手段と予めトランスポートストリームとは別の経路によって与えられる第3の鍵データ記憶手段と前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第1の鍵データ復号手段によって得られた第1の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備える。

【0025】ECM情報に変更があるまでは契約チャンネルを選局する毎に前記ECM記憶手段に記憶したECM情報を利用して前記第1の鍵データを抽出できる。また、ECM情報に変更された場合など、前記ECM記憶手段に記憶したECM情報を利用してデスクランブル処理ができない場合には、復調手段から新しくECM情報を抽出して更新して利用できる。ECMデータを一旦前記第2の鍵データ復号手段において復号することにより前記第2の鍵データを、ECMデータを一旦前記第1の鍵データ復号手段において復号することにより前記第1の鍵データを抽出できる。このECM記憶手段に記憶したECM情報より抽出した第1の鍵データを用いて前記デスクランブル手段によってデスクランブルすることで選局時間を短縮することができる。また、ECM情報やECM情報の更新頻度や送信頻度を低くした場合にも選局時間の短縮が可能である。

【0026】

【発明の実施の形態】以下本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の実施の形態について、実施例を用い、図面を参照して説明する。

【0027】図1は本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の一実施例を示すブロック図である。図1において、100は送信側暗号化変調装置、200はMPEG圧縮装置や

音声信号や映像信号を記憶しておくサーバなどを有する送信側映像信号源装置、300は暗号化鍵や顧客を管理するための送信側鍵等管理装置、400はCATV伝送路、500は受信側端末装置、600は映像音声表示器、700は郵送などの配送手段である。暗号化装置101は映像音声多重化及びコンテンツスクランブル回路111、112はスクランブル制御装置112、限定受信制御装置113から構成されている。時分割多重回路102はECM記憶回路121、ECM記憶回路122から構成されている。103は64QAM (Quadrature Amplitude Modulation) 変調回路、104は信号合成回路である。151は映像音声データ出力端子、152は第1の鍵データ出力端子、153は第2の鍵データ出力端子、154は第3の鍵データ出力端子、155は暗号化された第1の鍵データを含むECM (Entitlement Control Message) 情報出力端子、156は暗号化された第2の鍵データを含むECM (Entitlement Management Message) 情報出力端子、157はスクランブル映像音声データ出力端子、158はスクランブル映像音声、ECM情報、ECM情報多重データ出力端子、159は64QAMデジタル被変調波信号出力端子である。501は周波数多重信号分離回路、502は制御用マイコン、503は64QAM復調回路、504は誤り訂正回路、508はコンテンツデスクランブル回路、509はMPEG多重分離回路、510はMPEGビデオデコーダ、511はNTSC (National Television System Committee) ビデオエンコーダ、512はオーディオデコーダ、513はICカードなどの情報記憶媒体、514はECM記憶手段、515はECM記憶手段、505は鍵情報分離回路、506は第2の鍵復号回路、507は第1の鍵復号回路である。551は制御信号出力端子、552は64QAM被変調波信号出力端子、553は64QAM復調デジタルデータ出力端子、555は誤り訂正後デジタルデータ出力端子、556は暗号化された第1の鍵データ出力端子、557は暗号化された第2の鍵データ出力端子、558は第3の鍵データ出力端子、559は第2の鍵データ出力端子、560は第1の鍵データ出力端子、561はデスクランブルデジタルデータ出力端子、568はECM情報出力端子、569はECM情報出力端子、562は圧縮映像データ出力端子、564は映像データ出力端子、563は圧縮オーディオデータ出力端子、565はNTSCビデオ信号出力端子、566はアナログオーディオ信号出力端子である。

【0028】限定受信方式を有したケーブルテレビの送信装置は、送信側暗号化変調装置100、送信側映像信号源装置200および送信側鍵等管理装置300で構成され、送信側映像信号源装置200からの映像や音声の

データを含んだ映像音声データはMPEG2トランスポートストリーム形式あるいはトランスポートストリームに変換可能な形式のデジタルデータであり、端子151から暗号化装置101の映像音声多重化及びコンテンツスクランブル回路111に輸入される。映像音声データは映像音声多重化及びコンテンツスクランブル回路111で送信側鍵等管理装置300から出力された第1の鍵データによってトランスポートストリーム形式のデジタルデータを暗号化したスクランブル映像音声データとして端子157に出力され、時分割多重回路102に供給される。送信側鍵等管理装置300は第1の鍵データ152をスクランブル制御装置112へ送出し、第2の鍵データ153及び第3の鍵データ154を限定受信制御装置113へ送出する。スクランブル制御装置113は送信側鍵等管理装置300より受信した第1の鍵データ152を映像音声多重化及びコンテンツスクランブル回路111へ送出すると共に限定受信制御装置113より送られてくる第2の鍵データ153によって第1の鍵データ152を暗号化した後ECM情報の一部として時分割多重回路102へ送出する。この時第1の鍵データをスクランブル制御装置113に供給し、タイミングを制御しながら映像音声多重化及びコンテンツスクランブル回路111に供給しても良い。送信側鍵等管理装置300の端子153から取り出された第2の鍵データはスクランブル制御装置112に送出されると共に限定受信制御装置113に供給される。限定受信制御装置113において、第2の鍵データは送信側鍵等管理装置300の出力端子154から送られてくる第3の鍵データによって第2の鍵データを暗号化した後ECM情報の一部として時分割多重回路102へ送出する。時分割多重回路102には、端子155に取り出されたECM情報を記憶するECM記憶回路121と端子156に取り出されたECM情報を記憶するECM記憶回路122とが設けられており、それぞれの情報が更新されるまでは一旦記憶した情報を保持し、設定されたタイミングでECM記憶回路121とECM記憶回路122に記憶された情報である暗号化された第1の鍵データを含むECM情報、暗号化された第2の鍵データを含むECM情報とスクランブル映像音声データをトランスポートストリーム形式のデジタルデータとして時分割多重して、時分割多重装置102の端子158にスクランブル映像音声ECM情報、ECM情報多重データとして64QAM変調回路103に加えられる。なお、このECM情報、ECM情報は鍵情報だけを含む場合と、鍵情報のほかに他の情報、例えば契約情報などが含まれる場合がある。この他の情報は図示しない回路からスクランブル制御装置112及び限定受信制御装置113に供給される。

【0029】64QAM変調回路103ではスクランブル映像音声ECM情報、ECM情報多重データに誤り訂正用符号を付加し、インターリーブ処理及びエネルギー

拡散処理などを行なわれ、64QAMデジタル被変調波信号に変換されて端子159に出力される。この64QAMデジタル被変調波信号は信号合成回路104で他の64QAMデジタル被変調波信号やアナログ被変調波信号などと周波数多重されてCATV伝送路400に出力される。第3の鍵データ154は、ICカード等の情報記憶媒体513などによって郵送などの配送手段によって線路700を経由して限定受信方式を有したケーブルテレビの受信装置に配られる。

【0030】一方、限定受信方式を有したケーブルテレビの受信装置は、受信側端末装置500で構成される。受信側端末装置500では、周波数多重されて伝送された64QAMデジタル被変調波信号をCATV伝送路400から受ける。選局などの制御を行う制御用マイコン502の端子551に取り出された制御信号によって、この信号は周波数多重信号分離回路501で選局され、64QAM被変調波信号として端子552に取り出され、64QAM復調回路503に輸入される。64QAM復調回路503で64QAM被変調波信号は64QAM復調デジタルデータに復調され、端子553を介して誤り訂正回路504に供給され、ここで、伝送路で生じたデータの誤りが訂正される。誤り訂正後のデジタルデータは端子555を介してコンテンツデスクランブル回路508に輸入される。誤り訂正回路504ではインターリーブ処理やエネルギー拡散処理されたデータの復号も行なわれる。第1の鍵データ560が復号されるまではコンテンツデスクランブル回路508においてデスクランブルは実行されず、誤り訂正後デジタルデータはそのままMPEG分離回路509へ輸入される。MPEG分離回路509ではトランスポートストリーム形式で送られてきたECM情報及びECM情報を検出し、それぞれ端子569、568を通してECM記憶手段514及びECM記憶手段515へと送出される。ECM記憶手段514に記憶されたECM情報とECM記憶手段515に記憶されたECM情報は必要に応じて鍵情報分離回路505に送られる。鍵情報分離回路505は記憶されていたECM情報より暗号化された第1の鍵データを抽出して端子556に出力し、第1の鍵復号回路507へ送出する。また鍵情報分離回路505は記憶されていたECM情報より暗号化された第2の鍵データ557を抽出して端子557に出力し、第2の鍵復号回路506へ送出する。第2の鍵復号回路506では、郵送などの配送手段によって線路700を経由して入手したICカード等の情報記憶媒体513からの第3の鍵データを端子558に出力し、これによって暗号化された第2の鍵データを復号して端子559に第2の鍵データが得られる。第2の鍵データを第1の鍵復号回路507に供給することによって、第2の鍵データで暗号化された第1の鍵データを復号して端子560に第1の鍵データを得る。コンテンツデスクランブル回路508では、端子5

60から得られた第1の鍵データによって、暗号化されている誤り訂正後デジタルデータを復号して、MPEG2トランスポートストリーム形式のデスクランブルデジタルデータ561に戻す。MPEG多重分離回路509では圧縮映像データと圧縮オーディオデータに分離され、端子562には圧縮映像データが得られ、端子563には圧縮オーディオデータがえられ、それぞれMPEGビデオデコーダ510とオーディオデコーダ512に入力される。圧縮映像データはMPEGビデオデコーダ510によって映像データに変換され端子564に取り出され、NTSCビデオエンコーダ511によってNTSCビデオ信号に変換され、端子565からとりだされる。MPEG分離回路509の端子563に取り出された圧縮オーディオデータはオーディオデコーダ512に供給され、ここでアナログオーディオ信号に変換されて端子566に取り出される。このNTSCビデオ信号とアナログオーディオ信号は映像音声表示器600に入力されて、映像音声表示器600で表示された映像と音声などの情報を視聴者に提供できる。

【0031】以上のように、図1に示す実施例では、視聴者が契約したチャンネルを見る場合には、受信側端末装置500内部のECM記憶手段514及びEMM記憶手段515に記憶してあるECM情報や記憶してあるEMM情報を用いることによって、直ちに記憶してある暗号化された第1の鍵データ556を復号して、復号された第1の鍵データを得ることができる。従って、番組選択の都度あらためてECM情報やEMM情報を検出する必要はなく、その時間分だけ早く、コンテンツスクランブルを施した誤り訂正後デジタルデータをコンテンツデスクランブル回路508で復号して、MPEG2トランスポートストリーム形式のデスクランブルデジタルデータに戻すことができ、短時間で表示された映像と音声などの情報を得ることができる。

【0032】なお、本実施例において、電源投入とともにECM記憶手段514に全てのECM情報が記憶され、EMM記憶手段515に全てのEMM情報が記憶されるようにすることによって、第1の鍵データ、第2の鍵データを短時間で得ることが出来る。

【0033】また、選局要求に従って前記ECM記憶手段514に記憶されているECM情報より第1の鍵復号回路507によって復号された第1の鍵データを使用してコンテンツデスクランブル回路508でデスクランブルを行ってもスクランブルが解除できない場合には、改めてMPEG分離回路509よりECM情報を抽出し、ECM記憶手段514の記憶内容を更新すると共に、鍵情報分離回路505を通して第1の鍵復号回路507により得られた暗号化された第1の鍵データを第2の鍵データで復号することによって、コンテンツデスクランブル回路508においてデスクランブルが可能となる。一方、送信側でECM情報やEMM情報が更新され、受信

側端末装置500内部に記憶された更新前のECM情報やEMM情報が使用できなくなった場合には、時分割多重回路102においてECM情報やEMM情報の送出頻度を上げておけば比較的短時間で受信側端末装置500でECM情報やEMM情報を検出することができる。

【0034】なお、本実施例では、第1の鍵データから第3の鍵データまでの3種類の鍵データを用いたが、鍵の数には関係無く送信側鍵等管理装置300より更新及び送信される鍵の記憶・復号手段を受信側端末装置500内部に設けることによって短時間で選局動作を行うデジタル有線テレビジョン放送の限定受信方式を実現できる。一般的には、その鍵の数を増やすほど盗聴できにくいと言われている。

【0035】なお、本発明の実施例において、制御用マイコン502はECM情報やEMM情報が暗号化されているか否か、ECM情報やEMM情報が周波数多重分離回路501に入力されたか否かを監視すると共に画面上での契約状況を確認できるよう制御することができる。

【0036】図2は本発明によるケーブルテレビの限定受信システムに使用されるMPEG2トランスポートストリーム形式の信号構成を示す概念図である。図2において、2001はバケットヘッダであり、2002はMPEG映像データや音声データであり、ECM情報やEMM情報が含まれている。また、1チャンネルに複数、例えば4つの番組が多重されており、この番組を識別するためにSI情報が用いられる。2003は誤り訂正符号を示す。受信側端末装置500のMPEG2トランスポートストリーム形式に戻されたデスクランブルデジタルデータのデータの構成は、4バイトのバケットヘッダ2001と184バイトのMPEG映像データやMPEG音声データおよびECM情報やEMM情報のバケット2002で構成される。この4バイトのバケットヘッダ2001と184バイトのバケット2002で構成される188バイトのMPEG2トランスポートストリーム形式のデータに16バイトのリードソロモンと呼ばれる誤り訂正符号2003が付加されている。

【0037】図3は本発明によるケーブルテレビの限定受信システムに使用されるMPEG2トランスポートストリーム形式のバケットヘッダの信号構成を示す概念図である。図3において、3001は同期バイト、3002はトランスポートエラーインジケータ、3003はパイロードユニット開始インジケータ、3004はトランスポート優先度、3005はバケット識別子、3006はトランスポートスクランブル制御、3007はアダプテーションフィールド制御、3008は連続性指標を示す。図3は図2に示す4バイトのバケットヘッダ2001の詳細を示すもので、MPEGデータ2002に記載されるMPEG映像データやMPEG音声データおよびECM情報やEMM情報等のデータの内、特定の情報のバケットを検出するためのバケット識別子3005やこ

のMPEG映像データパケットにスクランブルが施されているかを示すトランスポートスクランブル制御3006などが付加されたものである。

【0038】図4は本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の他の実施例を示すブロック図である。図4において、520は第2の鍵データ記憶手段、521は第1の鍵データ記憶手段である。573は第2の鍵データ記憶手段520の出力端子であり、この端子573に記憶された第2の鍵データが出力される。572は第1の鍵データ記憶手段521の出力端子であり、この端子572に第1の鍵データ記憶手段521記憶された第1の鍵データが出力される。なお、図4において、図1と同じ機能を有するブロックには同一の符号を付けている。

【0039】受信側端末装置500では、周波数多重されて伝送された64QAMデジタル被変調波信号をCATV伝送路400から受け、周波数多重信号分離回路501で制御用マイコン502からの制御信号に応じて64QAM被変調波信号を選局する。この被変調波信号は64QAM復調回路503に入力される。64QAM復調回路503で64QAM被変調波信号は64QAM復調デジタルデータに復調され、端子553を通して誤り訂正回路504に供給され、この回路504で伝送路で生じたデータの誤りが訂正され、誤り訂正後デジタルデータとして端子555を通してコンテンツデスクランブル回路508に入力される。

【0040】誤り訂正回路504では、インターリーブ処理やエネルギー拡散処理されたデータの復号も行なう。第1の鍵データ560が復号されるまではコンテンツデスクランブル回路508においてデスクランブルは実行されず誤り訂正後デジタルデータはそのままMPEG分離回路509へ入力される。ここまでは図1に示した他の実施形態における動作と全く同様である。MPEG分離回路509ではトランスポートストリーム形式で送られてきたECM情報及びEMM情報を検出し、それぞれ端子569、568を通して鍵情報分離回路505に送る。鍵情報分離回路505は送られてきたECM情報より暗号化された第1の鍵データを抽出し、端子556を介して第1の鍵復号回路507へ送出する。また鍵情報分離回路505はMPEG分離回路509より送られてきたEMM情報より暗号化された第2の鍵データを抽出し、端子557を介して第2の鍵復号回路506へ送出する。郵送などの配送手段によって、伝送路700を経由して入手したICカード等の情報記憶媒体513から得られた第3の鍵データを端子558を介して第2の鍵復号回路506に供給する。第2の鍵復号回路506では第3の鍵データによって暗号化された第2の鍵データを復号することによって、第2の鍵データが得られる。この第2の鍵データは一旦第2の鍵データ記憶手段520に蓄えられた後端子573を介して第1の鍵復号

回路507へ送られる。第1の鍵復号回路507では第2の鍵データ記憶手段520より送られた第2の鍵データを用いて暗号化された第1の鍵データを復号して第1の鍵データが得られる。復号された第1の鍵データは第1の鍵データ記憶手段521に記憶された後、端子572を介してコンテンツデスクランブル回路508に送られる。以後、必要な場合は第1の鍵データ記憶手段521に記憶された第1の鍵データ572がコンテンツデスクランブル回路508に送られることになる。コンテンツデスクランブル回路508では、第1の鍵データ記憶手段521より送られた第1の鍵データを用いて、暗号化され且つ誤り訂正されたデジタルデータを復号して、MPEG2トランスポートストリーム形式のデスクランブルデジタルデータに戻され、MPEG多重分離回路509で圧縮映像データ562と圧縮オーディオデータ563に分離されてMPEGビデオデコード510とオーディオデコード512に入力される。

【0041】圧縮映像データはMPEGビデオデコード510によって映像データ564に変換され、NTSCビデオエンコーダ511によってNTSCビデオ信号に変換される。圧縮オーディオデータはオーディオデコード512によってアナログオーディオ信号に変換される。NTSCビデオ信号とアナログオーディオ信号はそれぞれ端子565、566を介して映像音声表示器600に入力されて、映像音声表示器600で表示された映像と音声などの情報を視聴者に提供できる。また、選局要求に従って第1の鍵データ記憶手段521より送られた第1の鍵データを使用してコンテンツデスクランブル回路508でデスクランブルできない場合には、改めてMPEG分離回路509よりECM情報を抽出し鍵情報分離回路505を通して第1の鍵復号回路507により暗号化された第1の鍵データを復号し、共に第1の鍵データ記憶手段521の内容を更新すると共に、第1の鍵データをコンテンツデスクランブル回路508に送信することでコンテンツデスクランブル回路508においてデスクランブルが可能となる。

【0042】図5は本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。図5において、102はECM情報を記憶して設定された頻度でトランスポートストリーム形式のデジタルデータとして時分割多重する時分割多重回路でありEMM情報の記憶手段は含んでいない。その他は図1と同じである。ケーブルテレビの送信側で限定受信システムにおける負荷の低減および違法受信対策のためEMM情報の送出頻度を低くする場合が考えられる。例えば、EMM情報の更新を1日に1回行うような場合には、EMM情報を常に送出すると伝送効率が下がる。よって、EMM情報の更新頻度が少ない場合にはEMM情報を常時送出する必要はない。この場合時分割多重回路102におけるEMM記憶

回路は必要ではなくなる。むしろ受信側端末装置500におけるECM記憶手段515において低い頻度で送信されるECM情報を記憶することにより、短時間でのスクランブルの解除が可能となる。なお、時分割多重回路102にECM記憶手段を設けな場合、ECM情報は外部装置、例えばパソコンを通して時分割多重回路102に入力されるため、ECM情報の送出頻度はこの外部装置の能力によって左右される。また、本実施例では受信側端末装置500の動作は図1に示した実施例と全く同様である。

【0043】図6は本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。図6において、102はECM情報を記憶して設定された頻度でトランスポートストリーム形式のデジタルデータとして時分割多重する時分割多重回路でありECM情報の記憶手段は含んでいない。520は第2の鍵データ記憶手段である。記憶された第2の鍵データは第2の鍵データ記憶手段520の端子573に取り出される。その他図1と同じ機能を有するブロックには同一の符号付けた。

【0044】受信側端末装置500では、周波数多重されて伝送された64QAMデジタル被変調波信号をCATV伝送路400から受け、周波数多重信号分離回路501で制御用マイコン502からの制御信号に応じて選局される。この選局された64QAM被変調波信号は64QAM復調回路503に入力される。64QAM復調回路503で64QAM被変調波信号は64QAM復調デジタルデータに復調され、誤り訂正回路504により伝送路で生じたデータの誤りが訂正される。誤り訂正されたデジタルデータはコンテンツデスクランブル回路508に入力される。誤り訂正回路504では、インターリーブ処理やエネルギー拡散処理されたデータの復号も行なわれる。第1の鍵データが復号されるまではコンテンツデスクランブル回路508においてデスクランブルは実行されず誤り訂正後デジタルデータはそのままMP

EG分離回路509へ入力される。MP

10

20

30

40

50

って、暗号化された第2の鍵データを復号して第2の鍵復号回路506の出力端子559に第2の鍵データが得られる。この第2の鍵データは一旦第2の鍵データ記憶手段520に蓄えられた後、第1の鍵復号回路507へ送られる。第1の鍵復号回路507では第2の鍵データ記憶手段520より送られた第2の鍵データを用いて暗号化された第1の鍵データを復号して、その出力端子560に第1の鍵データを得る。復号された第1の鍵データはコンテンツデスクランブル回路508に送られる。コンテンツデスクランブル回路508では、第1の鍵復号回路507より送られた第1の鍵データを用いて、暗号化されており、且つ誤り訂正されたデジタルデータを復号して、MP

EG2トランスポートストリーム形式のデスクランブルデジタルデータに戻され、MP

EG多重分離回路509で圧縮映像データと圧縮オーディオデータに分離され、それぞれMP

しくECM情報を抽出し、記憶されているECM情報を更新して利用できる。

【図面の簡単な説明】

【図1】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置の一実施例を示すブロック図である。

【図2】本発明の実施例を説明のためのMPEG2トランスポートストリーム形式の信号構成を示す概念図である。

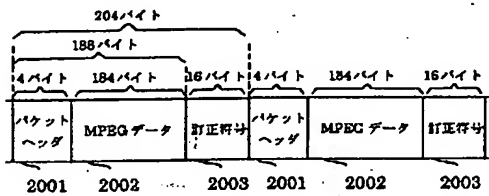
【図3】本発明の実施例を説明するためのMPEG2トランスポートストリーム形式のバケットヘッダの信号構成を示す概念図である。

【図4】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置の他の実施例を示すブロック図である。

【図5】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実

【図2】

図2



* 施例を示すブロック図である。

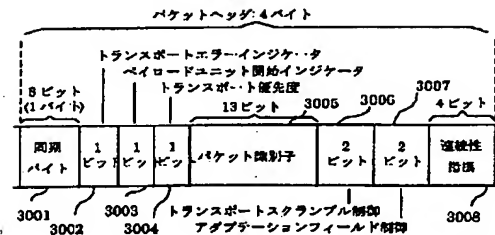
【図6】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。

【符号の説明】

100…送信側暗号化変調装置、200…送信側映像信号源装置、300…送信側鍵等管理装置、400…CATV伝送路、500…受信側端末装置、600…受信側TV受像機、101…暗号化装置、102…時分割多重回路、121…ECM記憶回路、122…EMM記憶回路、111…映像音声多重化及びコンテンツスクランブル回路、112…スクランブル制御装置、113…限定受信制御装置、503…64QAM復調回路、506…第2の鍵復号回路、507…第1の鍵復号回路、508…コンテンツデスクランブル回路、514…ECM記憶手段、515…EMM記憶手段。

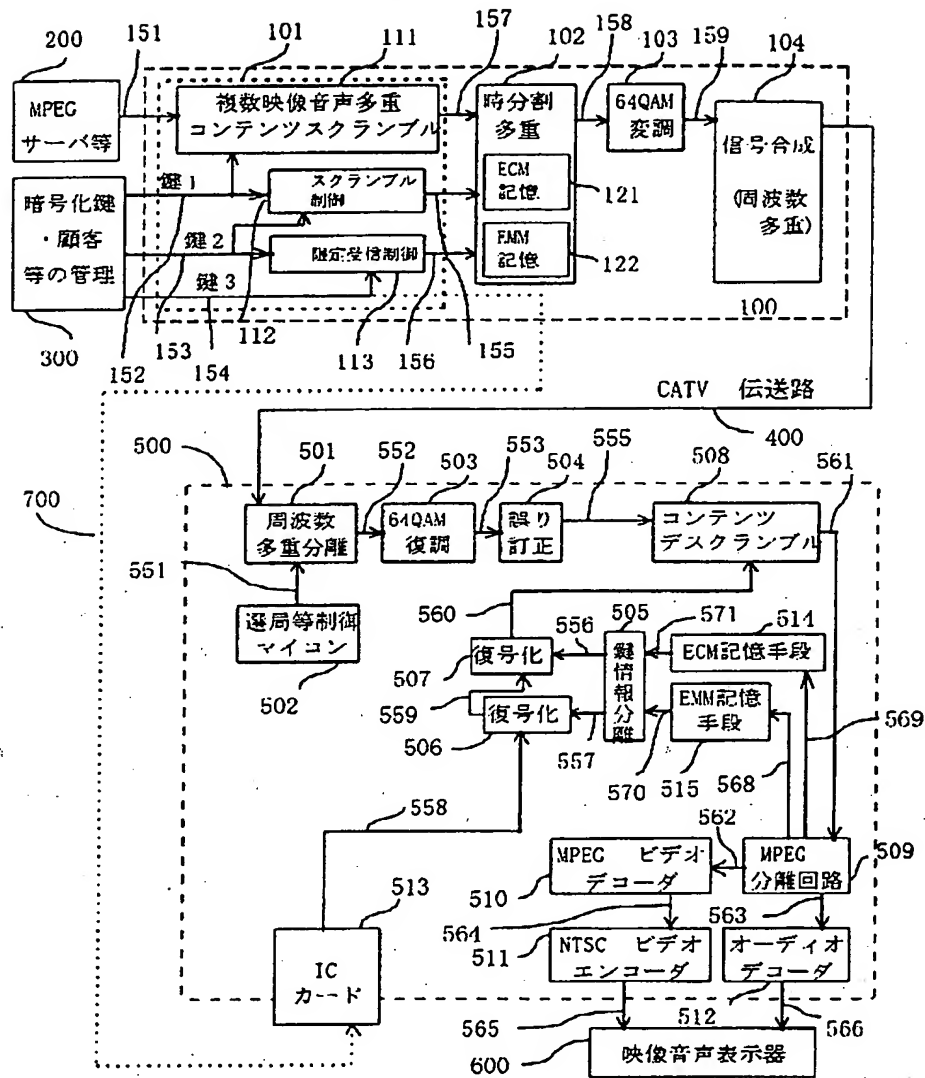
【図3】

図3



【図1】

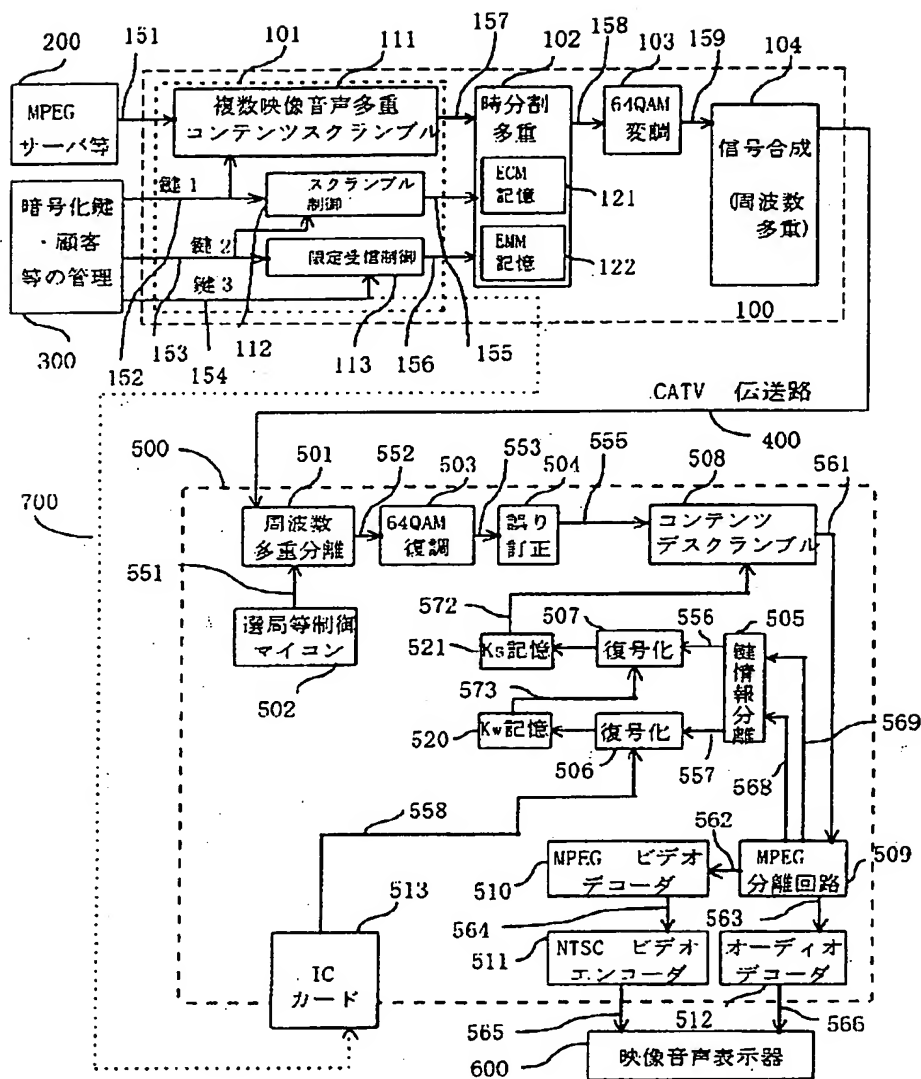
図 1



Best Available Copy

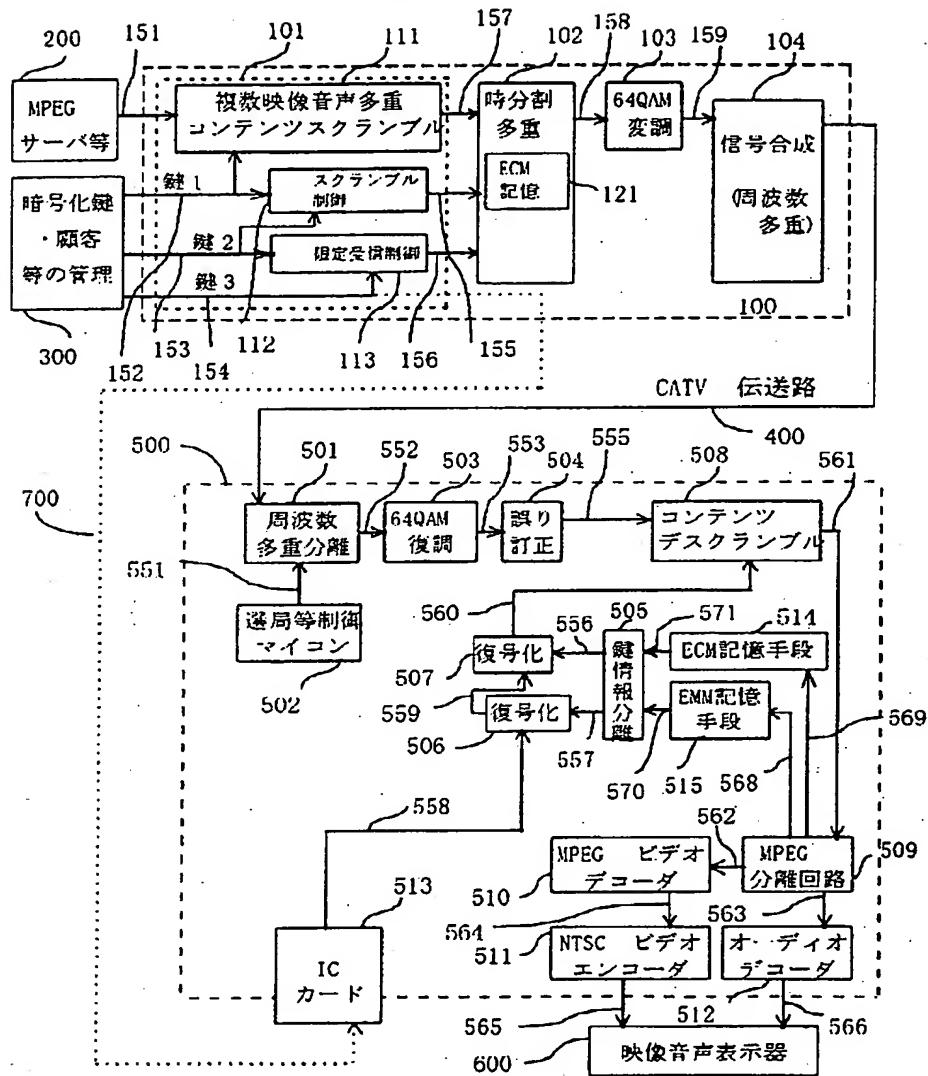
【図4】

図 4



【図5】

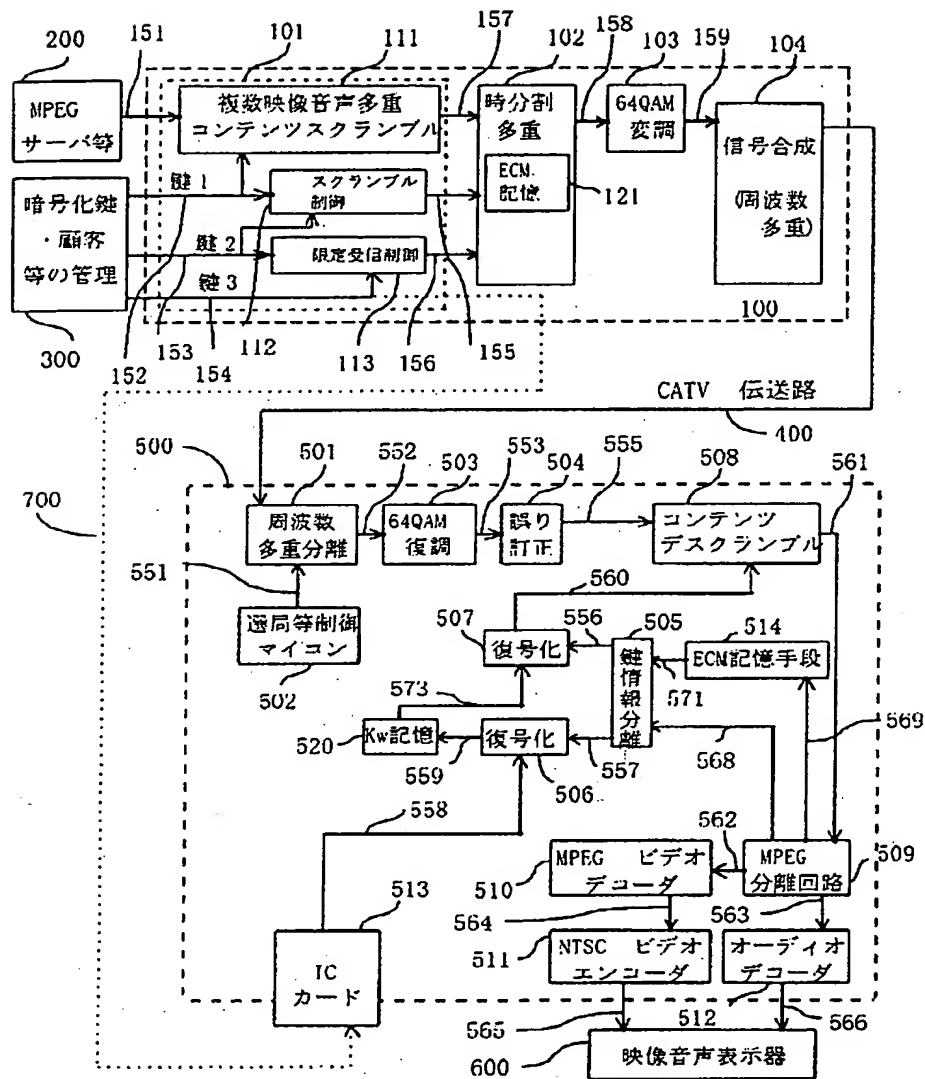
図 5



Best Available Copy

【図6】

図 6



フロントページの続き

(51) Int. Cl.

識別記号

F I

テーマコード(参考)

H 0 4 L 9/00

6 0 1 E

(72) 発明者 西田 正巳
 神奈川県横浜市戸塚区吉田町292番地 株
 式会社日立製作所A V事業部内

F ターム(参考) 5C064 BA01 BB02 BB05 BC16 BC17
 BC20 BC22 BD07 BD08 CA18
 CB01 CC01
 5J104 AA16 BA03 EA18 EA22 NA02
 NA35 PA06

Best Available Copy